LLNL Risk Management Approach

April 19, 2012

Rusty Babcock
Cyber Security

Lawrence Livermore National Laboratory

LLNL-PRES-549072

CS12-048

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

LLNL Approach to Risk Management Framework

- Risk Governance Model follows a centralized strategy that authorizes Laboratory Management to accept risks of operations for unclassified computer systems
  - Outlined in the National Institute of Standards and Technology (NIST), Special Publication 800-39 *Managing Information Security Risk*
  - Allows for one authorizing official under a common governance model
- Our strategy is for the Chief Information Officer to approve system operations including changes in risk
  - Removes the Livermore Site Office from the approval process for unclassified cyber systems
- Enables continuous operation of systems (ref. NIST 800-39)
  - Eliminates the need to rewrite security plans
  - Continuous monitoring
  - Change control process
    - In LLNL’s future is automated security plans
- Allows LLNL to tailor cyber defenses based on risk and implement common controls

LLNL Risk Management Status

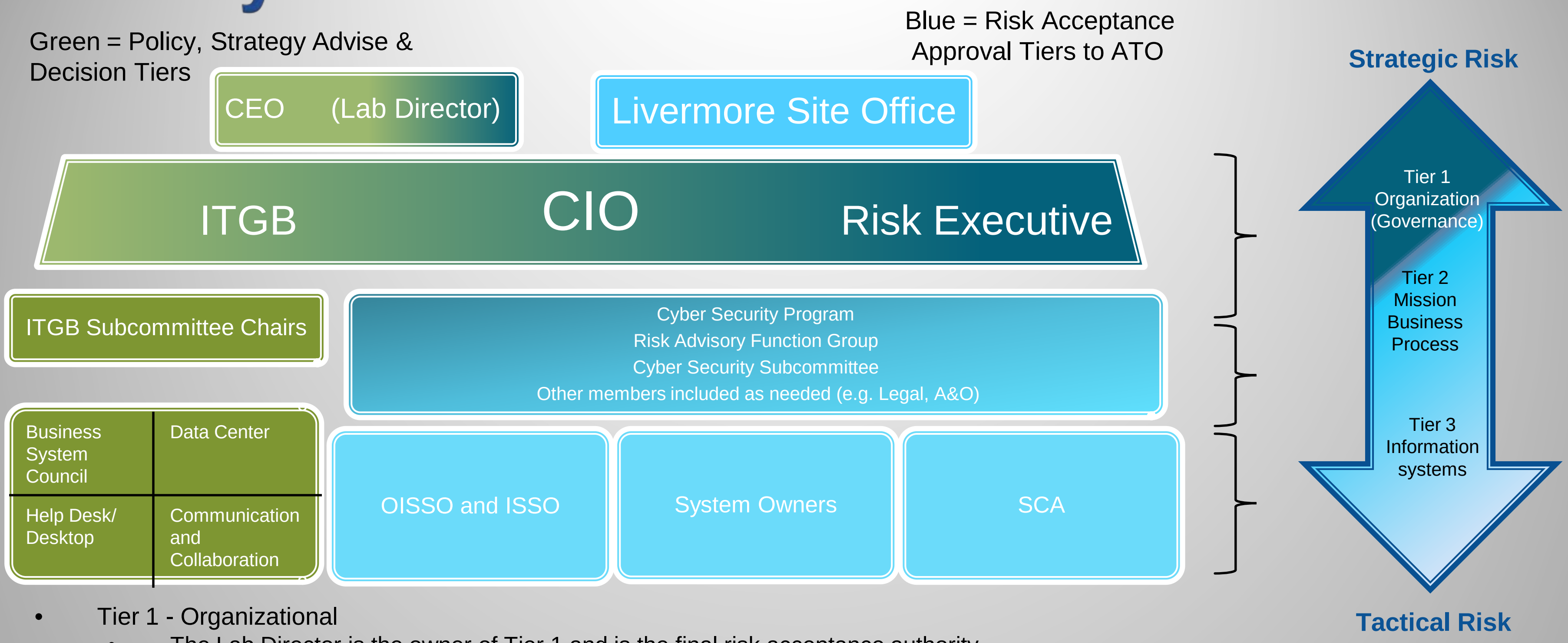
LLNL Risk Management Framework (RMF) objectives

- Implement the risk based approach and optimize the balance between mission needs, costs, and security
- Provide LLNL governance structure, processes, and policies for risk based cyber security management

Approach and Status

- Draft of Risk Management Governance document completed
- Risk Assessment methodology/procedures for: information systems, core services, and new technology at the institutional level in process
- Updated Common Controls document – describes security controls under new risk based framework in process
- ISSP Transition Plan in process
- Risk Acceptance Process – defines process and guidelines for Risk Executive to follow and accept residual risk in process
- RMF Contractor Assurance System (CAS) basic functionality in process
- Archer software installation to production in process
- Site Risk Agreement

Policy vs. Risk Tiers



Green = Policy, Strategy Advise & Decision Tiers

Blue = Risk Acceptance Approval Tiers to ATO

CEO (Lab Director)

Livermore Site Office

ITGB

CIO

Risk Executive

ITGB Subcommittee Chairs

Cyber Security Program
Risk Advisory Function Group
Cyber Security Subcommittee
Other members included as needed (e.g. Legal, A&O)

Business System Council

Data Center

Help Desk/ Desktop

Communication and Collaboration

OISSO and ISSO

System Owners

SCA

Strategic Risk

Tier 1 Organization (Governance)

Tier 2 Mission Business Process

Tier 3 Information systems

Tactical Risk

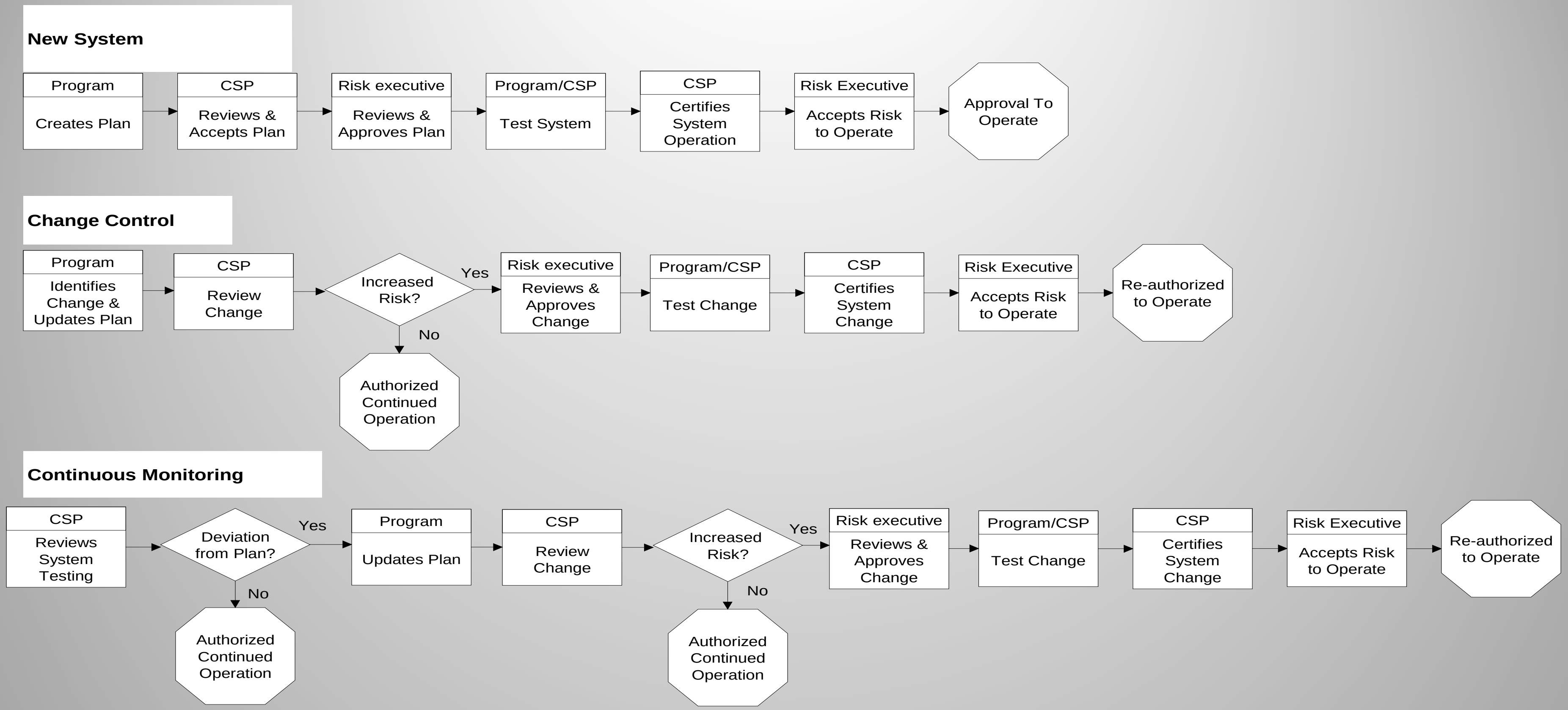
- Tier 1 - Organizational
  - The Lab Director is the owner of Tier 1 and is the final risk acceptance authority
  - Risk Executive function
    - Has the authority to accept the risk and is the Authorizing Official for information systems operation
    - The Chief Information Officer (CIO) is the Risk Executive by authority of the Lab Director
- Tier 2 - Mission/Business Processes
  - The Risk Advisory Function Group (RAFG)
    - Operates as a tactical advisory group to the Risk Executive
  - Cyber Security Subcommittee (CSS)
    - Supports RAFG
    - Provides recommendations to the CIO on acceptance of residual risk for Information System Security Plan (ISSP) and other institutional cyber security services
- Tier 3 - Information Systems
  - Cyber Security Program
    - Establishes and manages baseline policies and practices required of the LLNL classified and unclassified computer systems
    - Determines whether significant changes in the information systems or environments of operation require reauthorization

LLNL Risk Management Governance

- The concept of three tiers of Governance supports the system authorization
  - Tier 1 is the risk Executive Function and Tier 2 and Tier 3 support the Risk Executive in risk acceptance, determination, and advisory functions

- The three tiers have responsibilities for system authorization
  - Risk Management Acceptance process
    - Clearly defined to roles and decision points
    - High level process chart in Risk Management Governance Document
    - Risk Assessment Methodology provides input into Risk Management Acceptance process
      - Determine residual risk based on impact and probability

System Authorization



New System

Program: Creates Plan → CSP: Reviews & Accepts Plan → Risk executive: Reviews & Approves Plan → Program/CSP: Test System → CSP: Certifies System Operation → Risk Executive: Accepts Risk to Operate → Approval To Operate

Change Control

Program: Identifies Change & Updates Plan → CSP: Review Change → Increased Risk?

No → Authorized Continued Operation

Yes → Risk executive: Reviews & Approves Change → Program/CSP: Test Change → CSP: Certifies System Change → Risk Executive: Accepts Risk to Operate → Re-authorized to Operate

Continuous Monitoring

CSP: Reviews System Testing → Deviation from Plan?

No → Authorized Continued Operation

Yes → Program: Updates Plan → CSP: Review Change → Increased Risk?

No → Authorized Continued Operation

Yes → Risk executive: Reviews & Approves Change → Program/CSP: Test Change → CSP: Certifies System Change → Risk Executive: Accepts Risk to Operate → Re-authorized to Operate

- LLNL Risk Acceptance Process
  - New process implements system authorization through new Risk Executive
- Acceptance of residual risk
  - New systems flow through to the risk executive function
  - System changes flow to the appropriate level based on increase in residual risk
  - Continuous monitoring of existing system allows continued approval to operate

LLNL Risk Assessment Methodology

- Risk Assessment Methodology provides input into Risk Management Acceptance process
  - LLNL Methodology uses best practices from GRAM and NIST 800-30 and current LLNL Risk Assessment practices
- Two types of risk assessments integrated into one core process
  - Information System Security Plan (ISSP)
    - Identifying, prioritizing, and estimating information security risks associated with LLNL ISSPs
  - New or emerging technologies
    - Requests of management or from LLNL organization for the use of the new technology